

# Derandomizing quantum circuits with measurement based unitary designs

Peter S. Turner<sup>1,\*</sup> and Damian Markham<sup>2,†</sup>

<sup>1</sup>*School of Physics, H. H. Wills Physics Laboratory,  
Tyndall Avenue, University of Bristol, Bristol BS8 1TL, UK.*

<sup>2</sup>*CNRS LTCI, Departement Informatique et Reseaux, Telecom ParisTech,  
23 avenue d'Italie, CS 51327, 75214 Paris CEDEX 13, France*

(Dated: November 4, 2015)

Entangled multipartite states are resources for universal quantum computation, but they can also give rise to ensembles of unitary transformations, a topic usually studied in the context of random quantum circuits. Using several graph state techniques, we show that these resources can ‘derandomize’ circuit results by sampling the same kinds of ensembles quantum mechanically, (analogously to a quantum random number generator). Furthermore, we find simple examples that give rise to new ensembles whose statistical moments exactly match those of the uniformly random distribution over all unitaries up to order  $t$ , while foregoing adaptive feed-forward entirely. Such ensembles – known as  $t$ -designs – often cannot be distinguished from the ‘truly’ random ensemble, and so they find use in many applications that require this implied notion of pseudorandomness.

**Introduction** – Randomness is an important resource in both classical and quantum information theory, underpinning cryptography, characterisation, and simulation. Random unitary transformations are often considered in the form of random quantum circuits, with wide-ranging applications in, for example, estimating noise[1], private channels[2], modelling thermalisation[3], photonics[4], and even black hole physics[5]. Uniform randomness, sampling from the ‘flat’ Haar measure on a continuous group, is however very resource intensive. A natural definition of a less costly *pseudorandom* ensemble is one whose statistical moments are equal to those of the Haar ensemble up to some finite order  $t$  – this is the defining property of a  $t$ -design. Arising in classical coding theory[6], in the quantum community designs were first applied to states[7], and later to processes[8], the latter being our concern here. As mathematical objects they are of interest in their own right, not least of which as generalisations of SICPOVMs and MUBs which provide infamous open problems[9].

Rather than quantum circuits composed of sequences of gates, unitary transformations in a measurement based (MB) model[10] are realized by sequences of measurements on highly entangled resource states. These have random outcomes, and the resource states and measurement patterns can be chosen such that the result is an ensemble of unitary transformations[11]. Here we show that fixed graph states with deterministic measurement patterns can yield ensembles of unitary transformations on an arbitrary input that satisfy the  $t$ -design condition approximately *and* exactly. A connection between using classically randomised MB schemes to generate pseudorandomness (in the form of typical entanglement) and approximate unitary  $t$ -designs was mentioned in the optimization of random circuit constructions[12]. The advantage of inherent quantum randomness in MB schemes over random circuits was previously pointed out[13], also in the context of generating typical entanglement. We

see here this advantage extends to more general pseudorandomness –  $t$ -designs – in a natural way. In addition to the practical benefit of not requiring classical randomness and reconfiguration, the MB approach lends itself to new examples; we report exact MB 3-designs using only five and six qubits, within reach of current experiments, and give evidence of their novel mathematical structure.

**Approximate MB unitary designs** – Any universal model of computation allows one to implement an arbitrary ensemble of unitaries (or more general processes[14]) as follows. Consider sampling from the finite ensemble  $\{p_i, U_i\}$  ( $\sum_i p_i = 1$ ,  $p_i \geq 0$ ,  $U_i \in \text{U}(d)$  the set of  $d \times d$  unitary matrices), acting on an arbitrary input  $|\psi\rangle \in \mathbb{C}^d$ . A bipartite system in the state

$$\sum_i \sqrt{p_i} |i\rangle \otimes U_i |\psi\rangle, \quad (1)$$

is created by preparing first  $\sum_i \sqrt{p_i} |i\rangle \otimes |\psi\rangle$ , and then applying the controlled operation  $\sum_i |i\rangle\langle i| \otimes U_i$ . One then performs a projective measurement on the first part in the basis  $\{|i\rangle\}$ ; upon obtaining outcome  $j$ , unitary  $U_j$  is applied to the input, and this occurs with probability  $p_j$ . One way to generate pseudorandomness is therefore to take known unitary  $t$ -design ensembles and apply the above reasoning. What follows is based on the random circuit construction of Brandao, Harrow and Horodecki[15] (BHH) and shows that one can implement approximate  $t$ -designs efficiently using a MB scheme.

We briefly review the BHH construction. For any matrix  $\rho$  on the  $t$ -fold tensor product of  $\mathbb{C}^d$ , define its expectation with respect to the Haar measure  $dU$  as  $\mathbb{E}_H^t(\rho) := \int dU U^{\otimes t} \rho (U^{\otimes t})^\dagger$ , where the integral is performed over the entire unitary group  $\text{U}(d)$ . An ensemble of unitaries  $\{p_i, U_i\}$  is an approximate  $t$ -design if, for all  $\rho$ , the expectation is ‘close’ to that of the Haar ensemble:

$$(1 - \epsilon) \mathbb{E}_H^t(\rho) \leq \sum_i p_i U_i^{\otimes t} \rho (U_i^{\otimes t})^\dagger \leq (1 + \epsilon) \mathbb{E}_H^t(\rho), \quad (2)$$

where for matrices  $A \leq B$  if  $B - A$  is positive semidefinite, and  $\epsilon = 0$  for exact designs.

Consider a universal set of two-qubit gates  $\mathcal{U} \subset \text{U}(4)$ ; for technical reasons  $\mathcal{U} \ni U$  must contain its inverses  $U^\dagger$  and the matrix elements of each  $U$  must be algebraic. One constructs a “parallel” random circuit on  $n$  qubits in steps, at each step performing with probability  $1/2$  either the ‘even’ unitary  $U_{12} \otimes U_{34} \otimes \dots \otimes U_{n-1n}$ , or the ‘odd’  $U_{23} \otimes U_{45} \otimes \dots \otimes U_{n-2n-1}$ , where each  $U_{ij}$  is uniformly randomly sampled from  $\mathcal{U}$ . BHH show that for sufficiently many (polynomial in  $t$ ,  $n$  and  $1/\epsilon$ ) steps, the ensemble of such circuits is an  $\epsilon$ -approximate  $t$ -design.

Starting in an ‘even’ configuration, applying instead an ‘odd’ can be accomplished by a shift operation, defined over the  $n$  inputs and two ancilla qubits  $n+1$  and  $n+2$ ,

$$U_S := S_{n-2n+1} S_{n-1n+2} \prod_{i=1}^{n-2} S_{ii+1}, \quad (3)$$

where  $S_{ij} \in \text{U}(4)$  is the swap operation between qubits  $i$  and  $j$ . Iterating the circuit described in Fig. 1 therefore implements a random parallel circuit.

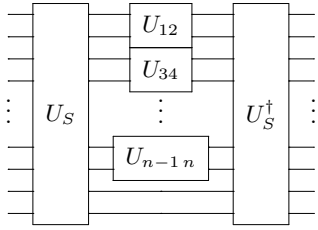


FIG. 1: One step in the random circuit construction of an approximate  $t$ -design over  $n$  qubits. The shift gate  $U_S$  and its inverse are together either randomly applied or not applied, with the two-qubit unitaries in between randomly sampled from the universal set  $\mathcal{U}$ . Polynomially many iterations of this random circuit will implement an approximate  $t$ -design[15].

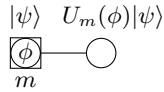


FIG. 2: The fundamental random unitary transformation induced by measurement on a graph state. Nodes are qubits initially prepared in the  $+1$  eigenstate  $|+\rangle$  of the Pauli  $X$  operator, and edges indicate entanglement via the controlled- $Z$  ( $CZ$ ) operation. Angles  $\phi$  indicate projective measurement direction in the Pauli  $XY$ -plane, with the random outcome bit  $m$ ; output nodes are unmeasured and therefore blank. Here we explicitly include an arbitrary input (square node) state  $|\psi\rangle$  and the output;  $U_m(\phi)$  is given by Eq. (4).

In the remainder of this section we will show how to implement this random parallel circuit with a MB scheme. The resource state in Fig. 2 (written as a graph, see caption) implements the random qubit unitary

$$U_m(\phi) := HZ^m Z(\phi), \quad (4)$$

where  $m \in \{0, 1\}$  is the random measurement outcome,  $H$  is the Hadamard matrix, and  $Z(\phi) := e^{-iZ\phi/2}$  (similar notation is used for Pauli  $X$  and  $Y$ ). Graphs can be connected (outputs of one identified with the inputs of the next) to perform products of unitaries. By connecting several copies of the graph in Fig. 2 and choosing measurement angles, Figs. 3 and 4 implement certain random one- and two-qubit unitaries, respectively.

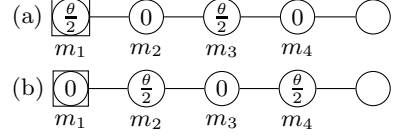


FIG. 3: By measuring the qubits as indicated, (a) implements randomly  $Z^{m_1 \oplus m_3} X^{m_2 \oplus m_4} Z(\theta)^{m_2 \oplus 1}$  while (b) implements randomly  $Z^{m_3} X^{m_2 \oplus m_4} X(\theta)^{m_3 \oplus 1} Z^{m_1}$ , where  $\oplus$  denotes bit-wise sum (ignoring unimportant global phases).

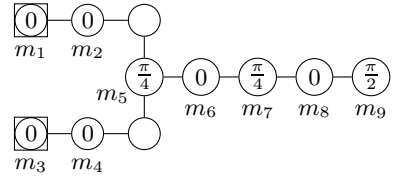


FIG. 4: Graph and measurement pattern implementing the two-qubit gate  $U_{ij} = (Z_i Z_j)^M (Z(\pi/2)_i Z(\pi/2)_j C Z_{ij})^{m_6 \oplus 1} \times X_i^{m_4} X_j^{m_2} Z_i^{m_3} Z_j^{m_1}$ , where  $M$  is a random bit which is a function of measurement results  $m_{5,7,8,9}$ .

These ‘gadgets’ can be combined to sample from a larger universal set of unitaries; Fig. 5 implements

$$U_{ij}^{\mathbf{M}} = (Z_i Z_j)^{M_1} (Z(\pi/2)_i Z(\pi/2)_j C Z_{ij})^{M_2} X_i^{M_3} X_j^{M_4} Z_i^{M_5} Z_j^{M_6} Z(\pi/4)_i^{M_7} Z(\pi/4)_j^{M_8} X_i^{M_9} X_j^{M_{10}} Z_i^{M_{11}} Z_j^{M_{12}} X(\pi/4)_i^{M_{13}} X(\pi/4)_j^{M_{14}} Z_i^{M_{15}} Z_j^{M_{16}}, \quad (5)$$

where, here and in the following,  $\mathbf{M}$  is a new bit string whose independently random entries are functions of the measurement results  $m_k$ . This set is universal because it contains the universal set  $\{X(\pi/4), Z(\pi/4), CZ\}$ ; note also that their matrix elements are algebraic. Furthermore, since  $ZX(\pi/4) = X(-\pi/4)Z$ , for every  $\mathbf{M}$  there exists an  $\mathbf{M}'$  such that  $U^{\mathbf{M}'} = (U^{\mathbf{M}})^{-1}$ , thus satisfying the conditions of the BHH construction.

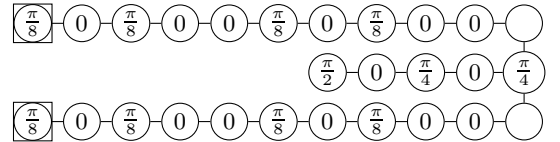


FIG. 5: Measurement gadgets combined in this way sample from a universal set of two-qubit unitaries, given in Eq.(5).

We can use these graph gadgets to implement the shift operator of Eq.(3). Each swap can be decomposed into  $CZ$  and  $H$  gates, which can in turn be decomposed as  $H = Z(\pi/2)X(\pi/2)Z(\pi/2)$ . The key observation is that in order to implement a random unitary composed of several gadget unitaries, we must correlate certain random outcomes. For example, if we naively combined gadgets to try to perform a random Hadamard as in Fig. 6(a), we would get the random unitary

$$X^{M_1} Z^{M_2} Z(\pi/2)^{M_3} X(\pi/2)^{M_4} Z(\pi/2)^{M_5}. \quad (6)$$

As we will see, the random Paulis on the left can be ignored; however, each of the three rotations are independently randomly applied, failing to implement  $H$  most of the time. We want to set  $M_3 = M_4 = M_5$ , and find that  $M_3 = m_2 \oplus 1$ ,  $M_4 = m_7 \oplus 1$  and  $M_5 = m_{10} \oplus 1$ , so this can be done by projecting qubits 2, 7 and 10 onto the same results in the  $X$  basis.

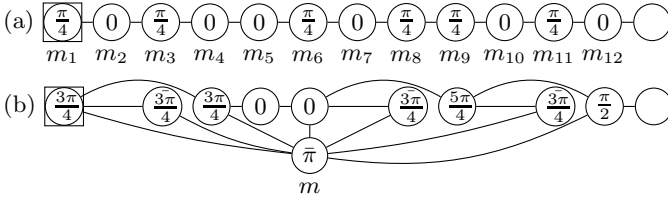


FIG. 6: (a) A naive random  $H$ , resulting in the unitary given in Eq.(6). (b) A random  $H$  where  $X$ -fusion has imposed common measurement results on the naive case, implementing  $X^M Z^{M'} H^m$  (the random Paulis are harmless;  $\bar{\phi}$  indicates measurements in the Pauli  $ZY$ -plane).

Projecting a set of vertices onto identical results can be accomplished by a new graph where the set is replaced with a single vertex in a particular way. In the case of common  $Z$  measurements on two qubits this is exactly the “fusion” operation of optical MBQC[16]. Here we require  $X$  ( $\phi = 0$ ) measurements to be correlated as these give rise to the crucial dependencies, and we call this graph transformation an  $X$ -fusion operation; see the appendix for details. In the case of the Hadamard example where the set of vertices to be correlated is  $\{2, 7, 10\}$ , the resulting graph is given in Fig. 6(b). Note that  $X$ -fusion introduces local Clifford operations that can change the measurement basis to the  $ZY$ -plane.

The random unitary resulting from Fig. 4 has unwanted  $Z(\pi/2)$  rotations correlated to the  $CZ$ . We can now use  $X$ -fusion to undo this: simply append  $Z(\pi/2)$  gadgets (Fig. 3(a)) and impose correlations using appropriate  $X$ -fusions, resulting in a new (rather complicated) graph. We assume this has been done in the following, where we combine these results to construct a graph that implements the random circuit of Fig. 1.

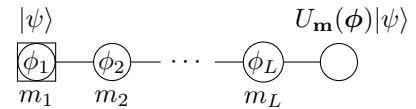
To find the graph for  $U_S$  we first decompose its circuit description into  $Z(\pi/2)$ ,  $X(\pi/2)$  and  $CZ$ . Where  $Z(\pi/2)$  and  $X(\pi/2)$  appear we use the gadgets of Fig. 3(a) and

(b) respectively, and where  $CZ$  appears we use the gadget of Fig. 4 (adapted as mentioned above). The same procedure can be used for  $U_S^\dagger$ . Between each pair of appropriate outputs of  $U_S$  and inputs of  $U_S^\dagger$  we insert the two-qubit gadget of Fig. 5. Looking at the induced unitaries corresponding to the gadgets (see figure captions), we see that, because the non-Pauli gates are Clifford, all the random Paulis can be moved to the left; this allows them to be absorbed into the randomly sampled two-qubit unitaries of Eq.(5), which remain universal. It remains to force all of the appropriate random  $U_S$  and  $U_S^\dagger$  outcomes to be the same; as in the Hadamard example of Eq.(6), ignoring Paulis we have the correct combination of rotations, apart from the fact that they occur independently. To correlate them we apply  $X$ -fusions on the appropriate qubits in each of the gadgets that make up the  $U_S$  and  $U_S^\dagger$  graphs. In this way we end up with a large graph, with fixed measurement angles prescribed by the gadgets, that implements the random parallel circuit of Fig. 1. Connecting such graphs effects repeated iterations of the random circuit as required.

It only remains to check that the graph does not scale badly in size or preparation time. The number of qubits used is polynomial in  $n$  because the number of gadgets used is linear in the number of BHH’s gates, and each gadget has a fixed number of nodes. The number of edges puts an upper bound on the preparation time. Each gadget has a fixed number of edges, and linearly many gadgets are used, so we need only be concerned with operations that change edges – the  $X$ -fusions. In the appendix we show that these can be chosen so that edges do not proliferate. In this way the number of edges is fixed for each gadget, so the total number of edges is linear in the number of gadgets, and therefore also in  $n$ .

This shows that fixed resource states with fixed measurement settings can give rise to pseudorandom ensembles in the form of approximate  $t$ -designs for all  $t$ ,  $n$  and  $\epsilon$ . The construction is efficient but requires a large overhead, which we expect can be greatly improved.

**Exact linear cluster designs** – We will now show that the MB approach can produce exact designs with surprisingly few resources. From Eq.(4) it follows that a linear cluster of  $L$  qubits



yields a unitary

$$U_{\mathbf{m}}(\phi) := U_{m_L}(\phi_L) \cdots U_{m_2}(\phi_2) U_{m_1}(\phi_1), \quad (7)$$

where  $\phi \in [0, \pi]^L$  and  $\mathbf{m} \in \{0, 1\}^L$  are ordered lists of angles and outcomes, respectively. Here node 1 is the input, and node  $L + 1$  is the output. We are interested in the ensemble of unitaries  $\{p_{\mathbf{m}}, U_{\mathbf{m}}(\phi)\}$  for all outcome

strings  $\mathbf{m}$ . The linearity of the cluster ensures that  $p_{\mathbf{m}} = 1/2^L$  will be the same for all  $\mathbf{m}$ , and since an ensemble has  $2^L$  elements the distribution is uniform.

A test for  $t$ -designness can be made using the *frame potential*[7, 18], which is a sum of powers of the ensemble elements' Hilbert-Schmidt overlaps. In our case of a uniform ensemble on qubits it is given by

$$F_L^t(\phi) := \frac{1}{4^L} \sum_{\mathbf{m}, \mathbf{m}'} |\text{Tr}[U_{\mathbf{m}}(\phi)^\dagger U_{\mathbf{m}'}(\phi)]|^{2t} \geq \frac{(2t)!}{t!(t+1)!}, \quad (8)$$

and the bound on the r.h.s. is known to be achieved if and only if the ensemble is a  $t$ -design. Equations (4,7) along with the cyclicity of the trace imply that the first and last measurement angles,  $\phi_1$  and  $\phi_L$ , do not affect the frame potential – note this does not mean the nodes themselves are redundant, since their measurement outcomes help to grow the ensemble. The frame potential is also symmetric under the transposition  $\phi_{l+1} \leftrightarrow \phi_{L-l}$ .

A  $t$ -design is by definition a  $(t-1)$ -design, and it is not hard to see that a 1-design must span the operator space, thus any design for the unitary group  $U(d)$  must contain at least  $d^2$  elements. Since here  $d = 2$  and the  $L = 1$  ensemble has but 2 elements, it cannot be a design. For  $L = 2$  the frame potential is easily computed:  $F_2^1(\phi) = 1$ , which coincides with the minimum in Eq. (8) for all  $\phi$  and is therefore always a 1-design, (choosing  $\phi = \{0, 0\}$  gives the Pauli ensemble up to phase). Any basis is a 1-design, and so we will subsequently concern ourselves with  $t \geq 2$ .

For  $L = 3$  the frame potential is  $F_3^2(\phi) = 2(1 + \cos^4 \phi_2 + \sin^4 \phi_2)$ , which has a global minimum of 3 at  $\phi_2 = \pi/4$ ; this exceeds the 2-design minimum of 2 from Eq. (8). This is not surprising, since there are 8 elements in the ensemble and a lower bound of 10 has been proved[19]. For  $L = 4$ , one finds the product  $F_4^2(\phi) = F_3^2(\phi_2)F_3^2(\phi_3)/4$ ; each factor can be independently minimised at angle  $\pi/4$ , yielding  $9/4 > 2$ . Thus even though there are more than the minimal number of elements, we have proved that for  $L = 4$  no choice of angles can give a 2-design, (and hence any  $(t \geq 2)$ -design).

For  $L = 5$  the frame potential can be written

$$F_5^2(\phi) = 4X_2X_4(x_3^2 + (3(1 - X_2^{-1})(1 - X_4^{-1}) - 1)x_3 + 1), \quad (9)$$

where  $X_2 := 1 - \cos^2 \phi_2 + \cos^4 \phi_2$ , similarly for  $X_4$ , and  $x_3 = \cos^2 \phi_3$ . This has a unique minimum of 2 at  $X_2 = X_4 = 3/4$  and  $x_3 = 1/3$ . Since this achieves the bound we do indeed have a 2-design, or more precisely a set of (intimately related) 2-designs as there are several choices of equivalent angles, the simplest being  $\phi_2 = \phi_4 = \pi/4$  and  $\phi_3 = \arccos \sqrt{1/3}$ .

One finds that this ensemble is also a 3-design;  $F_5^3(\phi_1, \pi/4, \arccos \sqrt{1/3}, \pi/4, \phi_5) = 5$ , again achieving the bound in Eq. (8). However, the  $t = 4$  value is

$14\frac{14}{27} > 14$ , and so it does not define a 4-design. We pause here to note that previous design constructions are predominantly related to group actions[18, 19], and in particular it is well known that 3-designs are generated by the Clifford group[8, 20]. One is led to ask whether or not the 32 unitary matrices (see appendix ) in this  $L = 5$  qubit 3-design also admit a finite group structure. Due to the irrationality of  $\phi_3$  however, any group containing the ensemble must have infinite order. Additionally, the number of ensemble elements for any such MB design must be a power of 2, which is not the case for Clifford designs. Thus it would seem that along with being practically motivated, MB designs are mathematically novel.

The following two facts are not hard to prove: if  $\{p_i, U_i\}$  is a  $t$ -design, then so is  $\{p_i, VU_iW\}$  for any  $V, W \in U(d)$ ; and the ensemble formed by the (uniform) union of a  $t$ -design and a  $t'$ -design is a  $\min(t, t')$ -design. Together they imply that once a MB  $t$ -design has been achieved, any choice of subsequent measurement pattern will output at least a  $t$ -design. Thus any measurement pattern including the subsequence  $\{1/2, 1/3, 1/2\}$  will remain a 3-design, where we have switched to a more natural parameterization  $\phi \rightarrow x = \cos^2 \phi$ . For  $L = 6$  calculations can still be carried out analytically, and interestingly a continuous family of 3-designs arises for angles given in the new parameterization by

$$\mathbf{x} = \left\{ x_1, \frac{1}{2}, x_3, \frac{3x_3 - 2}{3x_3 - 3}, \frac{1}{2}, x_6 \right\}, \quad x_3 \in \left[ 0, \frac{2}{3} \right]. \quad (10)$$

We can carry on the search for higher order designs in longer linear clusters, however the computational demands grow quickly and exact results are elusive. Figure 7 shows the difference  $\Delta F$  of the first seven frame potentials from the bound for linear clusters up to  $L = 10$ . Since the frame potential is the square of a 2-norm[18], one finds[21] that  $\sqrt{\Delta F}$  is an upper bound on the diamond norm definition of approximate  $t$ -designs used in Eq. (2). Thus a decreasing frame potential indicates a better approximate  $t$ -design, and there are several strategies for trying to minimize it. Figure 7 shows three such, discussed in the caption.

**Multi-qubit cluster designs** – The linear cluster results beg the question of the existence of exact MB designs for arbitrary graph states with multi-qubit inputs and outputs, in particular square lattice cluster states of  $N$  qubits in  $L$  layers. Note that the tensor product of two  $t$ -designs is *not* a  $t$ -design on the tensor product space, which can be seen by recognizing that such a tensor product will never reproduce the entangled correlations of the Haar ensemble. Thus, two linear cluster 2-designs such as those described above will not give a two-qubit 2-design, as some non-locality will have to be introduced. A square lattice cluster state can be viewed as doing so by introducing  $CZ$  gates between linear clusters. However, this does not introduce any new free parameters over which



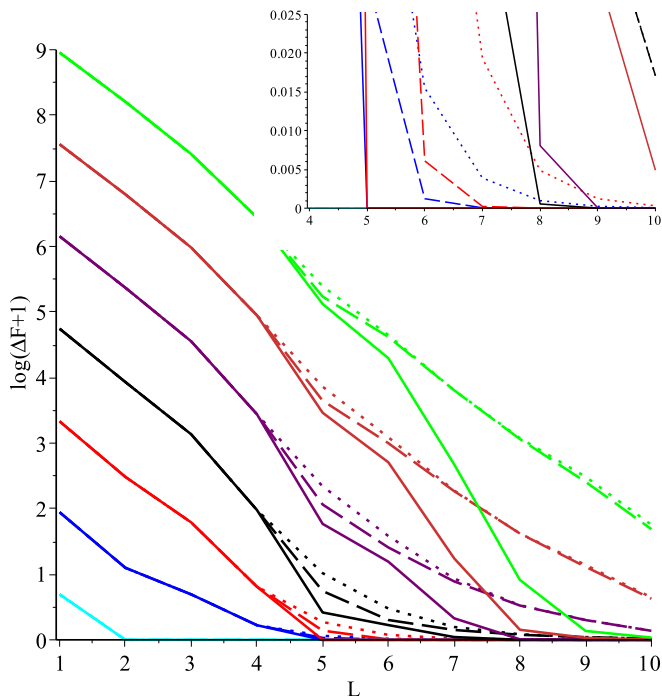


FIG. 7: From bottom to top the  $t = 1, \dots, 7$  frame potentials (interpolated), given by the difference  $\Delta F$  from the exact bound (logarithmic scale) versus linear cluster length  $L$ . For each we consider three measurement patterns: dotted lines for those consisting entirely of the angle  $\pi/4$ ; dashed lines for those consisting of a single measurement angle  $\phi_{\min}$  that minimizes the frame potential; and solid lines for a full multi-angle minimization (performed in Matlab). One sees that the former approach the bound exponentially, albeit with a decreasing rate, as predicted by random quantum circuit results[22]. The latter can be seen to drop much more quickly beyond  $L = 4$ . Other than the trivial  $t = 1$  case, only the  $t = 2, 3$  curves reach  $\Delta F = 0$  (inset), *i.e.* the exact design for  $L = 5$ . Despite the  $t = 4, 5$  curves coming very close to zero, an analytic solution at  $L = 9$  has not been found[23].

we can try to optimize the pseudorandomness of the output ensemble (*e.g.* minimize a frame potential) – it only introduces non-locality in a very rigid way. Unfortunately this makes it impossible to find small examples of exact multi-qubit designs. A numerical exploration of the problem shows that the same general behaviour, (exponential convergence to the Haar value, as in Fig. 7), is exhibited by square clusters, but the complexity of the computation prohibits an extensive search. Clearly the way forward is to identify a (likely group) structure in the ensembles that can be exploited in the multi-qubit case; the exact results above are a major step in this direction, but further investigation is required.

**Conclusion** – We have shown that there exist MB resources that produce arguably the most randomness possible in the form of approximate and exact  $t$ -designs. This arises despite no classical randomness being injected into the system; they are fixed graph states with a deterministic measurement pattern, outputting ensembles

that are sampled quantum mechanically.

The role of  $t$ -designs in quantum estimation[24], in particular randomized benchmarking[1], along with cluster states being an important model for error corrected quantum computation in realistic hardware, leads one to anticipate MB designs being useful in the near future. Related work has recently been done where ancillas in a random circuit model are used to realize exact 2-designs with a quadratic improvement in resources[25]. This work demonstrates a new method for finding useful designs, that could make use of powerful MB techniques such as gFlow[26]. The broad question raised is, *what resource states provide the most (pseudo)randomness most efficiently?* In this direction it is intriguing to note that the MB approach can give rise to probability distributions that are impossible to efficiently sample classically[27], leading one to imagine MB resources that outperform classical randomization in principle as well as in practice. Several generalizations come to mind, including arbitrary graphs, qudit nodes, non-standard resource preparations (*e.g.*  $> 2$ -body entangling gates), and weighted designs. We hope this work motivates further research into these and other possibilities.

**Acknowledgements** – The authors would like to thank D. Gross, D. Mahler, T. Rudolph, A. Doherty, A. B. Sainz, A. Scott, A. Roy and S. Bartlett for helpful discussions. PST acknowledges support from an EPSRC First Grant, US ARO Grant No. W911NF-14-1-0133, and a School of Physics travel grant. DM acknowledges support from ANR grant COMB and ville de Paris grant CiQWii.

\* Electronic address: peter.turner@bristol.ac.uk

† Electronic address: markham@enst.fr

- [1] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd and D. G. Cory. Science, 302(5653):2098, (2003); J. M. Epstein, A. W. Cross, E. Magesan, and J. M. Gambetta, Phys. Rev. A 89, 062321 (2014).
- [2] P. Hayden, D. Leung, P. W. Shor and A. Winter, Comm. Math. Phys. 250, 371, (2004).
- [3] M. P. Muller, E. Adlam, L. Masanes and N. Wiebe, Comm. Math. Phys. 340, 499 (2015).
- [4] J. C. F. Matthews, R. Whittaker, J. L. O'Brien and P. S. Turner, Phys. Rev. A 91, 020301(R) (2015).
- [5] P. Hayden and J. Preskill, J. High E. Phys. 2007(09), 120 (2007).
- [6] P. Delsarte, J. Goethals, and J. Seidel, Geom. Dedicata, vol. 6, pp. 363 (1977).
- [7] J.M. Renes, R. Blume-Kohout, A. J. Scott and C. M. Caves, J. Math. Phys. 45, 2171 (2004).
- [8] C. Dankert, R. Cleve, J. Emerson and E. Livine, Phys. Rev. A 80, 012304 (2012).
- [9] D. M. Appleby, C. A. Fuchs and H. Zhu, Q. Info. & Comp. 15, 61 (2015); T. Durt, B-G. Englert, I. Bengtsson and K. Zyczkowski, Int. J. Quant. Info. 8, 535 (2010).
- [10] R. Raussendorff and H. J. Briegel, Phys. Rev. Lett. 86,

- 5188 (2001).
- [11] M. Mhalla, M. Murao, S. Perdrix, M. Someya and P. S. Turner, [arXiv:1006.2616](#).
  - [12] W. G. Brown, Y. S. Weinstein and L. Viola, Phys. Rev. A 77, 040303(R) (2008).
  - [13] A.D. Plato, O.C. Dahlsten and M.B. Plenio, Phys. Rev. A 78, 042332 (2008).
  - [14] M. Nielsen and I. Chuang, “Quantum Computation and Quantum Information,” Cambridge 2000.
  - [15] F.G.S.L. Brandao, A.W. Harrow and M. Horodecki, [arXiv:1208.0692](#).
  - [16] D. Browne and T. Rudolph, Phys. Rev. Lett. 95, 010501 (2005).
  - [17] M. Hein, J. Eisert and H. J. Briegel, Phys. Rev. A 69, 062311 (2004).
  - [18] D. Gross, C. Audenaert and J. Eisert, J. Math. Phys. 48, 052104 (2007).
  - [19] A. Roy and A. J. Scott, Des. Codes Cryptogr. 53, 13-31 (2009).
  - [20] P. S. Turner, Proceedings, Nankai Series in Pure, App. Math. and Theo. Phys. 11, World Scientific, 2013; R. Kueng and D. Gross, [arXiv:1510.02767](#).
  - [21] R. A. Low, PhD thesis, University of Bristol, (2010) [arXiv:1006.5227](#).
  - [22] J. Emerson, E. Livine and S. Lloyd, Phys. Rev. A 72, 060302(R) (2005)
  - [23] Conversely, proving the *nonexistence* of exact designs should be possible using sum-of-squares techniques for bounding the global minima of polynomials, because these have semi-definite programming certificates; however, the problem seems to be numerically unstable and we were unable to coax convincing bounds on the frame potential from SOSTools ([www.cds.caltech.edu/sostools/](http://www.cds.caltech.edu/sostools/)).
  - [24] A. J. Scott, J. Phys. A: Math. Theor. 41, 055308 (2008).
  - [25] R. Cleve, D. Leung, L. Liu and C. Wang, [arXiv:1501.04592](#).
  - [26] D. E. Browne, E. Kashefi, M. Mhalla and S. Perdrix, New J. Phys. 9 250 (2007).
  - [27] M. Hoban, J. Wallman, H. Anwar, N. Usher, R. Raussendorf and D. Browne, Phys. Rev. Lett. 112, 140505 (2014).
  - [28] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A 69, 022316 (2004); Phys. Rev. A 70, 034302 (2004).

## APPENDIX

**Generalised fusion operations**– In order to have correlated random unitaries in a measurement based (MB) scheme, we wish certain measurement results to be correlated. Say we want to impose the same result on vertices  $A = \{a\}$ . To do this, we can think of replacing those vertices with a single vertex,  $\alpha$ , whose measurement outcome will be this correlated result. This is done by applying the following projector

$$\sum_m |m\rangle_\alpha \langle m, m, \dots, m|, \quad (11)$$

where  $m$  is the measurement result, and  $\{|m\rangle_\alpha\}_m$  is the measurement basis on vertex  $\alpha$ . When the measurement

basis is Pauli, it turns out this operation can be understood in terms of graph rewrite rules as a generalisation of the “fusion” operation[16]. For our gadgets the measurement results that should coincide will always be in the  $X$  basis.

It is useful to review the graphical notation we are using in a more formal way [17, 26]. Start with a graph  $G$  composed of vertices  $V$  and edges  $E$ . Each vertex  $v \in V$  represents a qubit. Certain vertices represent the inputs  $I \subset V$  (identified by having a box around them) whose qubits are in some state  $|\psi\rangle_I$ . Non-input vertices represent qubits initialised in the state  $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$ . Edges  $E$  represent the application of control- $Z$  gates ( $CZ$ ). This is sometimes called the open graph state,

$$|G(\psi)\rangle_V = \prod_{(ij) \in E} CZ_{ij} |\psi\rangle_I |+\dots+\rangle_{V/I}. \quad (12)$$

To perform a computation, non-output vertices are measured along angles in the Pauli  $XY$ -plane[26]; the simplest example is given in Fig. 2. In order to make a MB computation deterministic, corrections are made to account for random outcomes. For example, doing the correction  $Z^m H$  on Eq.(4) would implement the deterministic unitary  $Z(\phi)$ . In our situation however we do not want to correct for the measurement results – indeed they are the source of randomness for our ensembles.

Another way of describing the open graph state of Eq.(12) is via its stabilisers, defined for all noninput vertices  $a \notin I$  as

$$K_a = X_a \bigotimes_{b \in N(a)} Z_b, \quad (13)$$

where  $N(a)$  indicates the set of neighbours of vertex  $a$ . Open graph states satisfy the stabiliser equations

$$K_a |G(\psi)\rangle = |G(\psi)\rangle. \quad (14)$$

We will also make use of the squareroot stabilisers  $\sqrt{K_a} := X(\pi/2)_a \bigotimes_{b \in N(a)} Z(\pi/2)_b$ . The following operation takes an open graph state to a new one in which the graph given by the local complementation

$$T_a := \bigotimes_{b \in N(a)} Z_b \sqrt{K_a}. \quad (15)$$

The local complementation of a graph around vertex  $a$ , denoted  $\tau_a$  is given by complementing its neighbourhood, *i.e.* if two neighbours of  $a$  are connected in the original graph, they become disconnected, and vice versa. This operation is used extensively in quantum information processing using graph states[17],

$$T_a |G(\psi)\rangle = |\tau_a(G)(\psi)\rangle. \quad (16)$$

We begin by considering fusions in the case where all the measurements are in the  $Z$  basis, which is a simple extension of the two qubit fusion introduced in [16].

In the case of the other Pauli measurements, local complementation is used to jump between bases as done in [17, 28]. We will only consider fusion projections occurring on non-inputs, and furthermore they will only have non-input neighbours; that is  $A \notin I$  and  $N(A) \notin I$ . This is so that the stabiliser relations can be suitably applied, and allows us to treat graphs with no inputs in the proofs for simplicity.

We start with a simple expansion for any graph state,

$$|G\rangle_V = \sum_{\mathbf{m}} |\mathbf{m}\rangle_A \prod_{a \in A} Z_{N(a)}^{m_a} |g\rangle_{V/A}, \quad (17)$$

where here the  $|\mathbf{m}\rangle_A$  is a product state in the computational basis for bit string  $\mathbf{m}$  of length  $|A|$ ,  $g$  is the subgraph given by removing all the vertices in  $A$  and attached edges,  $m_a$  is the measurement outcome for node  $a$ , and  $Z_{N(a)}$  is shorthand for applying  $Z$  on the vertices  $N(a)$ . We define the  $Z$  basis fusion on vertices  $A$  as

$$F_Z^A := |0\rangle_{\alpha A} \langle 00 \cdots 0| + |1\rangle_{\alpha A} \langle 11 \cdots 1|. \quad (18)$$

From the expansion Eqn. (17), it is clear that this has the effect

$$F_Z^A |G\rangle = \sum_m |m\rangle_{\alpha} Z_{\Delta_{a \in A} N(a)}^m |g\rangle_{V/A}, \quad (19)$$

where  $\Delta_{a \in A} N(a)$  denotes the  $n$ -fold symmetric difference over the sets  $N(a)$ ,  $a \in A$  [11]. Graphically this is just the set of vertices which are connected an odd number of times to  $A$ . The resulting state is also a graph state, found in two steps. First add a new vertex  $\alpha$  and connect it to the odd neighbourhood of  $A$  (again, this is given by the symmetric difference of all the neighbours of  $a \in A$ ). Second remove vertices  $A$  and all their edges. We denote the new graph as  $F_Z^A(G)$ . In the case that  $A = \{a_1, a_2\}$  is composed of two vertices, the new graph is found by simply replacing the two vertices by a new vertex  $\alpha$  which is connected to the neighbours of  $a_1$  and  $a_2$ , minus the

neighbours common to both. See for example Fig. 8. This is exactly the fusion operation used in [16].

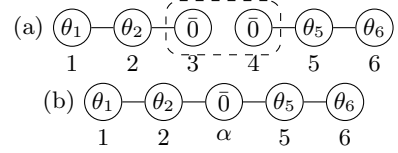


FIG. 8: Example of the  $Z$  fusion operation, where vertices 3 and 4 are to be  $Z$ -fused. A bar indicates measurements in the  $ZY$ -plane (hence  $\bar{0}$  represents a  $Z$  basis measurement). Thus, measuring vertices  $A = \{3, 4\}$  in the  $Z$  basis in graph (a) and imposing the same results is equivalent to measuring vertex  $\alpha$  in the  $Z$  basis in graph (b).

To see how the remaining Pauli basis fusions work, we use the fact that the bases can be related to each other by Clifford operations, which in turn can be mapped to graphical operations through local complementation [17]:

$$\begin{aligned} |+\rangle &= Y(\pi/2)|0\rangle \\ &= e^{-i\pi/4} Z(-\pi/2) X(-\pi/2) |0\rangle \\ |-\rangle &= Y(\pi/2)|1\rangle \\ &= -ie^{-i\pi/4} Z(-\pi/2) X(-\pi/2) |1\rangle \\ |+i\rangle &= X(-\pi/2)|0\rangle \\ |-i\rangle &= -iX(-\pi/2)|1\rangle, \end{aligned} \quad (20)$$

where  $|\pm(i)\rangle := (|0\rangle \pm (i)|1\rangle)/\sqrt{2}$ . So for the  $X$  fusion projection  $F_X^A := |+\rangle_{\alpha A} \langle ++ \cdots +| + |-\rangle_{\alpha A} \langle - \cdots -|$ , we have

$$F_X^A = Y(\pi/2)_{\alpha} Z(-\pi|A|/2) F_Z^A \bigotimes_{a \in A} X(\pi/2)_a Z(\pi/2)_a. \quad (21)$$

To relate this to the local complementation of Eq. (16), we note that for two non-input neighbours  $a, b \notin I$ ,

$$X_a(\pi/2) Z_a(\pi/2) = \left( Y_a \otimes X_b(-\pi/2) Z_b(\pi/2) \bigotimes_{c \in N(a) \Delta N(b)} Z_c(\pi/2) \bigotimes_{d \in N(a) \cap N(b)} Z_d \right) T_a T_b, \quad (22)$$

where  $A \Delta B$  indicates the symmetric difference between sets  $A$  and  $B$ . Then we observe that  $F_Z^A \bigotimes_{a \in A} Y_a = i^{|A|} X_{\alpha} Z_{\alpha}^{|A|} F_Z^A$ . Next, for each vertex  $a \in A$  we choose a neighbour  $b^a \in N(a)$ . If this can be done such that

$b^a \notin A$  and  $N(b^a) \cap A = a$  (as is the case for all our gadgets – in other cases similar rules can be found using the same reasoning),  $F_X^A$  can be given the simple form

$$F_X^A = Y(\pi/2)_\alpha Z(\pi|A|/2)_\alpha X_\alpha \prod_{a \in A} \left( X_{b^a}(-\pi/2) Z_{b^a}(\pi/2) \bigotimes_{c \in N(a) \Delta N(b^a)} Z_c(\pi/2) \bigotimes_{d \in N(a) \cap N(b^a)} Z_d \right) F_Z^A \prod_{a \in A} T_a T_{b^a}. \quad (23)$$

Similarly, for  $Y$ -fusion

$$\begin{aligned} F_Y^A &= X(\pi/2)_\alpha Z(-\pi|A|/2)_\alpha F_Z^A \bigotimes_{a \in A} X(\pi/2)_a \\ &= T_\alpha Z(-\pi|A|/2)_\alpha F_Z^A \prod_{a \in A} T_a. \end{aligned} \quad (24)$$

Remembering that  $T_a$  has the effect of implementing a local complementation, the above can be used to find the graphical rules for the fusion projections. Up to local unitaries, the graphs after the  $X$  and  $Y$  fusions are

$$F_X^A(G) = F_Z^A(\circ_{a \in A} (\tau_a \circ \tau_{b^a \in N(a)}(G))), \quad (25)$$

$$F_Y^A(G) = F_Z^A(\circ_{a \in A} (\tau_a(G))), \quad (26)$$

where  $\circ_{a \in A}$  indicates the composition of operations over  $A$ .

Thus  $X$ -fusion has the effect of changing the graph and applying local unitaries. An example of an  $X$ -fusion can be found in Fig. 9. The graph changes according to the the local complementation rules of Eq. (25). The local unitaries are given by Eq. (23):

$$\begin{aligned} &Z_1(\pi/2) \\ &X_2(-\pi/2) Z_2(\pi/2) \\ &X_5(-\pi/2) Z_5(\pi/2) \\ &Z_6(\pi/2) \\ &Y_\alpha(\pi/2) Z_\alpha X_\alpha. \end{aligned} \quad (27)$$

In the figure these are represented by changes to the measurement angles. Note that the  $X_2(-\pi/2) Z_2(\pi/2)$  rotate the axis of measurement from the  $XY$ -plane to the  $ZY$ -plane.

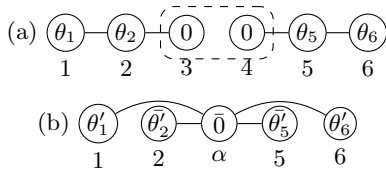


FIG. 9: Example of an  $X$  fusion operation. Here,  $\theta'_v := \theta_v + \frac{\pi}{2}$ , and again a bar indicates measurement in the  $ZY$ -plane. Vertices 3 and 4 in (a) are fused according to Eq. (25), resulting in (b) with local unitaries indicated above. Thus, measuring vertices  $A = \{3, 4\}$  in the  $X$  basis in graph (a) and imposing the same results is equivalent to measuring vertex  $\alpha$  in the  $Z$  basis in (b).

**Scaling of approximate MB  $t$ -designs** – First we note that the number of nodes in the MB construction is linear in the number of qubits in the BHH circuit construction. This can be seen by noting that the shift operation of Eq. (3) involves  $n + 2$  swap operations, each of which can be decomposed into 3  $CZ$  and 6  $H$  gates, and the latter further decomposes into 3 rotations, giving a total of 21 gadgets per  $U_S$  (and similarly  $U_S^\dagger$ ). Furthermore, each  $U_{ij}$  in Fig. 1 corresponds to a single (appropriately  $X$ -fused) gadget. Since the number of nodes in any gadget is fixed, the total number of nodes in the MB graph is linear in  $n$ .

We also want to show that the  $X$ -fusion operations do not introduce inefficiencies in the preparation of the graph states. Since the number of qubits goes down in the fusion operation, we are only concerned with making sure the number of edges does not grow too quickly. The only way that the number of edges could grow is if the local complementations of one gadget affect other gadget graphs. It turns out that for the vertices  $a \in A$  in the fused set we can choose  $b \in N(a)$  in such a way to avoid this. Concretely, if we consider the local complementations that occur for our gadgets, we can do the following. For Fig. 3(a) we have  $a = 2$  and use  $b = 3$ , for Fig. 3(b) we have  $a = 3$  and use  $b = 2$ , and for Fig. 4 we have  $a = 6$  and use  $b = 7$ . Since in each case neither vertex is an output, the complementations do not ‘reach’ beyond the gadget.

BHH show that the random circuit of Fig. 1 applied polynomially many times gives an approximate  $t$ -design. More precisely, they show there exists a constant  $C(\mathcal{U})$ , which depends on the universal set of gates  $\mathcal{U}$  used, such that repeating the circuit in Fig. 1  $C(\mathcal{U})[\log_2(4t)]^2 t^5 t^{3.1}(nt + \log(1/\epsilon))$  times forms an  $\epsilon$ -approximate  $t$ -design. Applying this to our measurement based graph state construction where we use a particular universal set, and recalling that the graph state size scales linearly with  $n$ , we arrive at the following assertion:

The graph construction presented, with the fixed measurement settings detailed, samples from an  $\epsilon$ -approximate  $t$ -design. Furthermore, there exists a constant  $C$  such that the size of the graph is  $C[\log_2(4t)]^2 t^5 t^{3.1}(nt + \log(1/\epsilon))$ .

**Minimal exact linear cluster design** – The 32 elements of the (essentially) unique  $L = 5$  MB 3-design:



$$\begin{aligned}
& \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \\
& \frac{1}{\sqrt{2}} \left\{ \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} i & -i \\ -i & -i \end{bmatrix}, \begin{bmatrix} -i & -i \\ i & -i \end{bmatrix} \right\}, \\
& \frac{1}{\sqrt{3}} \left\{ \begin{bmatrix} -1 & 1+i \\ 1-i & 1 \end{bmatrix}, \begin{bmatrix} 1-i & 1 \\ -1 & 1+i \end{bmatrix}, \begin{bmatrix} 1+i & i \\ i & 1-i \end{bmatrix}, \begin{bmatrix} i & 1-i \\ 1+i & i \end{bmatrix} \right\}, \\
& \frac{1}{\sqrt{6}} \left\{ \begin{bmatrix} -i & 2+i \\ -2+i & i \end{bmatrix}, \begin{bmatrix} -2+i & i \\ -i & 2+i \end{bmatrix}, \begin{bmatrix} -1-2i & -1 \\ -1 & 1-2i \end{bmatrix}, \begin{bmatrix} -1 & 1-2i \\ -1-2i & -1 \end{bmatrix}, \right. \\
& \quad \begin{bmatrix} \sqrt{3}-i & -1+i \\ 1+i & \sqrt{3}+i \end{bmatrix}, \begin{bmatrix} 1+i & \sqrt{3}+i \\ \sqrt{3}-i & -1+i \end{bmatrix}, \begin{bmatrix} -1+i & -1+i\sqrt{3} \\ -1-i\sqrt{3} & 1+i \end{bmatrix}, \begin{bmatrix} -1-i\sqrt{3} & 1+i \\ -1+i & -1+i\sqrt{3} \end{bmatrix}, \\
& \quad \left. \begin{bmatrix} 1-i\sqrt{3} & -1-i \\ -1+i & -1-i\sqrt{3} \end{bmatrix}, \begin{bmatrix} -1+i & -1-i\sqrt{3} \\ 1-i\sqrt{3} & -1-i \end{bmatrix}, \begin{bmatrix} -1-i & \sqrt{3}-i \\ -\sqrt{3}-i & -1+i \end{bmatrix}, \begin{bmatrix} -\sqrt{3}-i & -1+i \\ -1-i & \sqrt{3}-i \end{bmatrix} \right\}, \\
& \frac{1}{\sqrt{12}} \left\{ \begin{bmatrix} \omega_+ & \omega_- + 2i \\ \omega_- - 2i & -\omega_+ \end{bmatrix}, \begin{bmatrix} \omega_- - 2i & -\omega_+ \\ \omega_+ & \omega_- + 2i \end{bmatrix}, \begin{bmatrix} 2+i\omega_- & -i\omega_+ \\ -i\omega_+ & 2-i\omega_- \end{bmatrix}, \begin{bmatrix} -i\omega_+ & 2-i\omega_- \\ 2+i\omega_- & -i\omega_+ \end{bmatrix}, \right. \\
& \quad \left. \begin{bmatrix} -i\omega_- & -2-i\omega_+ \\ 2-i\omega_+ & i\omega_- \end{bmatrix}, \begin{bmatrix} 2-i\omega_+ & i\omega_- \\ -i\omega_- & -2-i\omega_+ \end{bmatrix}, \begin{bmatrix} \omega_+ + 2i & -\omega_- \\ -\omega_- & -\omega_+ + 2i \end{bmatrix}, \begin{bmatrix} -\omega_- & -\omega_+ + 2i \\ \omega_+ + 2i & -\omega_- \end{bmatrix} \right\}, \quad (28)
\end{aligned}$$


---

where each row is an orthonormal Hilbert-Schmidt basis, and we've defined  $\omega_{\pm} = \sqrt{3} \pm 1$ . Ensembles resulting from the removal of any basis fail to be a 2-design.

**Partial recursion for the frame potential** – The ensemble elements' Hilbert-Schmidt overlaps

$$\langle\langle \mathbf{m} | \mathbf{m}' \rangle\rangle_{\phi} := \text{Tr} [U_{\mathbf{m}}(\phi)^{\dagger} U_{\mathbf{m}'}(\phi)], \quad (29)$$

define a  $2^L \times 2^L$  Gram matrix. Substituting Eq.(4) into Eq.(7) one finds that due to reductions to previous cases, the important upper triangular Gram elements are of the form  $\langle\langle 0\mathbf{m}0 | 1\mathbf{m}'1 \rangle\rangle$ , where now  $\mathbf{m}, \mathbf{m}'$  are bit strings of length  $L-2$  and the angular dependence is implicit. Let  $\phi_k^l = \phi_k, \phi_{k+1}, \dots, \phi_{k+l-1}$  and define

$$f^t(\phi_2^{L-2}) := 2 \sum_{\mathbf{m}} \left( |\langle\langle 0\mathbf{m}0 | 1\mathbf{m}1 \rangle\rangle|^{2t} + 2 \sum_{\mathbf{m}' > \mathbf{m}} |\langle\langle 0\mathbf{m}0 | 1\mathbf{m}'1 \rangle\rangle|^{2t} \right) \quad (30)$$

(recall that the angles  $\phi_1$  and  $\phi_L$  are irrelevant for the frame potential). Combined with the diagonal ( $f^t = 0$ ) cases  $F_1^t = 4^t/2$  and  $F_2^t = 4^t/4$ , one arrives at a partially recursive formula for the frame potential:

$$\begin{aligned}
F_{L+1}^t(\phi_2^{L-1}) &= 2^{-1} \left[ F_L^t(\phi_2^{L-2}) + F_L^t(\phi_3^{L-2}) \right] \\
&\quad - 2^{-2} F_{L-1}^t(\phi_3^{L-3}) + 2^{-2L-1} f^t(\phi_2^{L-1}). \quad (31)
\end{aligned}$$

This can be used to reduce the complexity of frame potential calculations, and can give insight into their minimisation.